REMARKS

Claims 1-29 are pending in this application. Claims 1, 5, 6, 8-11, 16, 20, and 29 have been amended. Support for the claim amendments can be found in the specification and the accompanying drawings. No new matter has been added. Favorable reconsideration and allowance of the pending claims are respectfully requested.

Claim Objections

Claims 1 and 11 stand objected to based on claim informalities. Applicant respectfully submits that claims the amendments to claims 1 and 11 overcome the objections set forth in the Office Action. Accordingly, reconsideration and withdrawal of the claim objections is respectfully requested.

Claim Rejections - 35 U.S.C. § 103(a)

Claims 1-29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent Publication Number (USPPN) 2003/0051041 to Kalavade et al. ("Kalavade") in view of USPPN 2003/0046589 to Gregg et al. ("Gregg"). Applicant respectfully traverses this rejection.

To render a claim obvious under 35 U.S.C. § 103(a), there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the reference (or references when combined) must teach or suggest all the claim limitations. *See e.g.*, MPEP § 2143. Further, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

While Applicant disagrees with the § 103(a) rejection, independent claims 1, 5, 11, 16, and 20 have been amended in order to advance prosecution on the merits. For example, among their other elements, amended independent claims 1 and 11 recite a method of establishing a protected communications channel with a trusted code module

executing in a trusted execution environment in an open platform of a computing system ... and providing access to a service by the open platform of the computing system using the SIM AAA capabilities in the trusted execution environment of the computing system.

Amended independent claim 5 recites:

> establishing a protected communications channel with a trusted code module executing in a protected execution environment in an open platform of a computing system;
>
> using subscriber identity module (SIM) capabilities provided by the computing system in the protected execution environment without a discrete hardware SIM device for user authorization, authentication and accounting in association with a subscription account; and
>
> providing a subscription account service for access by the open platform of the computing system using the SIM capabilities in the protected execution environment of the computing system.

Amended independent claim 16 recites:

> establishing a protected communications channel with a trusted code module executing in a trusted execution environment in an open platform of a computing system;
>
> authenticating and authorizing a user of a subscription account at least in part by using Subscriber Identity Module (SIM) compliant authentication and authorization capabilities on a trusted execution environment in the open platform of the computing system that provides the SIM-compliant authentication and authorization capabilities without use of a discrete SIM hardware device; and
>
> providing user access to the subscription account upon receipt of predetermined credentials.

Amended independent claim 20 recites:

> a server having access to a network; and
> a provisioning module stored on the server, the provisioning module, when executed by the provisioning server, to establish a protected communications channel with a trusted module executing in a trusted execution environment in an open platform of a computing system and participate in provisioning Subscriber Identity Module (SIM) secret data from the server to the trusted execution environment, the computing system to provide SIM-compliant authentication, authorization, and accounting capabilities without use of a discrete hardware SIM device, and the server to provide access to a service by the computing system using the SIM-compliant authentication, authorization and accounting capabilities in the trusted execution environment of the computing system.

As noted in the Office Action, Kalavade fails to teach or suggest a trusted environment in an open platform of a computer system as recited by amended independent claims 1, 5, 11, 16, and 20. To address the admitted deficiencies of Kalavade, the Office Action relies on portions of Gregg disclosing:

> ...This finger print is also called an integrity metric or cryptographic digest. Once this metric is available, it is saved in the TPM's secure memory location. During the PC boot progress, other integrity metrics are collected from the PC platform, for instance finger prints of the boot loader and the operating system itself...
>
> ... The protected storage of the TPM is essentially non-volatile storage that has means of access control. This access control determines which entities (e.g., user, programs, etc.) have permission to read, write, modify and update the secure memory of the TPM. It is assumed that protected storage has some form of access control protocol that is used to protect against certain kinds of attack.

Gregg arguably discloses a hardware device known as the Trusted Platform Module (TPM) that includes non-volatile storage as means for access control, and the access control determines which entities have permission to read, write, modify, and update the secure memory within the TPM. Applicant submits that Gregg fails to teach or suggest a method of establishing a protected communications channel with a trusted code module executing in a trusted execution environment in an open platform of a computing system, as recited by amended independent claims 1 and 11. Further, Applicant submits Gregg also fails to teach or suggest providing access to a service by

the open platform of the computing system using the SIM AAA capabilities in the trusted execution environment of the computing system.

With respect to amended independent claim 5, Gregg also fails to teach or suggest "establishing a protected communications channel with a trusted code module executing in a protected execution environment in an open platform of a computing system; using subscriber identity module (SIM) capabilities provided by the computing system in the protected execution environment without a discrete hardware SIM device for user authorization, authentication and accounting in association with a subscription account; and providing a subscription account service for access by the open platform of the computing system using the SIM capabilities in the protected execution environment of the computing system."

With respect to amended independent claim 16, Gregg also fails to teach or suggest "establishing a protected communications channel with a trusted code module executing in a trusted execution environment in an open platform of a computing system; authenticating and authorizing a user of a subscription account at least in part by using Subscriber Identity Module (SIM) compliant authentication and authorization capabilities on a trusted execution environment in the open platform of the computing system that provides the SIM-compliant authentication and authorization capabilities without use of a discrete SIM hardware device; and providing user access to the subscription account upon receipt of predetermined credentials."

With respect to amended independent claim 20, Gregg also fails to teach or suggest "a provisioning module stored on the server, the provisioning module, when executed by the provisioning server, to establish a protected communications channel with a trusted module executing in a trusted execution environment in an open platform of a computing system and participate in provisioning Subscriber Identity Module (SIM) secret data from the server to the trusted execution environment, the computing system to provide SIM-compliant authentication, authorization, and accounting capabilities without use of a discrete hardware SIM device, and the server to provide access to a service by the computing system using the SIM-compliant authentication, authorization and accounting capabilities in the trusted execution environment of the computing system."

In view of the above, even if Kalavade and Gregg could be combined, which Applicant does not admit, such combination would not teach or suggest all the features of amended independent claims 1, 5, 11, 16, and 20. Further, Applicant submits that there is no teaching, suggestion or motivation to modify Kalavade and/or Gregg to include all the features of amended independent claims 1, 5, 11, 16, and 20. Consequently, Kalavade and Gregg, whether taken alone or in combination, are insufficient to render amended independent claims 1, 5, 11, 16, and 20 obvious under § 103(a).

For at least the above reasons, Applicant submits that amended independent claims 1, 5, 11, 16, and 20 are allowable and dependent claims 2-4, 6-10, 12-15, 17-19, and 21-29 are also allowable by virtue of their dependency from allowable claims, as well as on their own merits.

Conclusion

It is believed that claims 1-29 are in allowable form. Accordingly, a timely Notice of Allowance to this effect is earnestly solicited.

Applicant does not otherwise concede, however, the correctness of the rejection set forth in the Office Action with respect to any of the features of the independent claims and dependent claims. Accordingly, Applicant hereby reserves the right to make additional arguments as may be necessary to further distinguish the claims from the cited references, taken alone or in combination, based on additional features contained in the independent claims or dependent claims that were not discussed above. A detailed discussion of these differences is believed to be unnecessary at this time in view of the basic differences in the independent claims pointed out above.

The Examiner is invited to contact the undersigned at 724-933-9344 to discuss any matter concerning this application.

The Office is hereby authorized to charge any additional fees or credit any overpayments under 37 C.F.R. § 1.16 or § 1.17 to Deposit Account 50-4238

.

Respectfully submitted,

KACVINSKY LLC

/Robert V. Racunas/

Robert V. Racunas, Reg. No. 43,027
Under 37 CFR 1.34(a)

Dated: October 23, 2008

KACVINSKY LLC
C/O Intellevate
P.O. Box 52050
Minneapolis, MN 55402
(724) 933-5529